CYBER INCIDENT RESPONSE TEAM

DESCRIPTION	The Cyber Incident Response Team responds to crises or urgent situations within the pertinent cyber domain to address, manage, and mitigate immediate and potential threats.
RESOURCE CATEGORY	Cybersecurity
RESOURCE KIND	Team
OVERALL FUNCTION	The Cyber Incident Response Team: 1. Investigates and analyzes all relevant cyber and network activities related to the crisis situation with the purpose of achieving the speediest recovery of the impacted critical infrastructure service 2. Uses mitigation, preparedness, response, and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security 3. Documents all steps and actions taken during the operations and develops Incident Action Reports (IAR)
COMPOSITION AND ORDERING SPECIFICATIONS	1. Discuss logistics for deploying this team, such as working conditions, length of deployment, security, lodging, transportation, and meals, prior to deployment 2. The requestor may need to order multiple teams to provide 24 hour coverage 3. A single source entity may constitute the entire team 4. The requestor should specify if the personnel should have training and experience with specific software applications, hardware, and equipment

Each type of resource builds on the qualifications of the type below it. For example, Type 1 qualifications include the qualifications in Type 2, plus an increase in capability. Type 1 is the highest qualification level.

COMPONENT	SINGLE TYPE	NOTES
MINIMUM PERSONNEL PER TEAM	15	Not Specified
MANAGEMENT AND OVERSIGHT PERSONNEL PER TEAM	2 - National Incident Management System (NIMS) Type 1 Cyber Incident Responder	Not Specified
SUPPORT PERSONNEL PER TEAM	1 - NIMS Type 2 Cyber Incident Responder 3 - NIMS Type 1 Computer Network Defense (CND) Analyst 1 - NIMS Type 1 CND Infrastructure Support Specialist 1 - NIMS Type 2 CND Infrastructure Support Specialist 1 - NIMS Type 1 Database Administration Specialist 1 - NIMS Type 1 Digital Forensics Specialist 1 - NIMS Type 2 Digital Forensics Specialist 1 - Voice Communications Operator 1 - System Administrator 2 - Network Administrator	1. All members of the team should hold an active security clearance. 2. Any use of the term "forensics" is descriptive of a skill or capability and does not imply a law enforcement role. 3. The Voice Communications Operator, System Administrator, and Network Administrator are not NIMS typed support positions.

COMPONENT	SINGLE TYPE	NOTES
OPERATIONS EQUIPMENT PER TEAM	13 - Laptops with wireless internet card and programs for creation of documents, spreadsheets, and databases 2 - Laptops with a digital forensics tool suite 2 - Write-block hardware devices 2 - Devices capable of live memory capture	1. Team may need additional equipment and supplies for small local area network interfaces to tactical outbound communications. 2. An understanding of asset information including operating systems, key applications, incident response plans, organization charts, emergency contact lists, and hardware is essential prior to deploying team, to ensure team brings the appropriate tools. 3. Iterations of training deployments determine additional software and hardware items to conduct forensics, network analysis, and other supporting functions.
COMMUNICATIONS EQUIPMENT PER TEAM MEMBER	1 - Cell phone	Consider alternate forms of communication, such as satellite phones, based on the mission assignment and team needs.

NOTES

Nationally typed resources represent the minimum criteria for the associated component and capability.

REFERENCES

1. FEMA, NIMS 509: CND Analyst
2. FEMA, NIMS 509: CND Infrastructure Support Specialist
3. FEMA, NIMS 509: Cyber Incident Responder
4. FEMA, NIMS 509: Database Administration Specialist
5. FEMA, NIMS 509: Digital Forensic Specialist
6. FEMA, National Incident Management System (NIMS), October 2017
7. U.S. Department of Homeland Security, National Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework, v.2, May 2014